Method and device for producing an encrypted payload data stream and method and device for decrypting an encrypted payload data stream

Abstract

In a method for producing an encrypted method payload data stream comprising a header and a block containing encrypted payload data, a payload data key for a payload data encryption algorithm for encrypting payload data is generated. The payload data is encrypted using the generated payload data key and the payload data encryption algorithm to obtain the block containing the encrypted payload data of the payload stream. A part of the payload data stream is processed to deduce information marking the part of the payload data stream. The information is linked with the payload data by means of an invertible logic linkage to obtain a basic value. This basic value is finally encrypted using a key of two keys being different from each other by an asymmetrical encryption method, the two different keys being the public and the private keys respectively for the asymmetrical encryption method to obtain an output value being an encrypted version of the payload data key. The output value is finally entered into the header to complete the payload stream. Changes of the header and of the payload data itself, which are not authorized, lead to an automatic destruction of the payload data.